Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERTA

Paris, le 01 décembre 2006
N° CERTA-2006-AVI-522

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités de Xerox WorkCenter

Gestion du document

Référence	CERTA-2006-AVI-522
Titre	Multiples vulnérabilités de Xerox WorkCenter
Date de la première version	01 décembre 2006
Date de la dernière version	–
Source(s)	
Pièce(s) jointe(s)	Aucune

TAB. 1 – *Gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

- Exécution de code arbitraire à distance ;
- contournement de la politique de sécurité.

2 Systèmes affectés

- *Xerox Workcentre*, versions 232, 238, 245, 255, 265, 275 ;
- *Xerox Workcentre Pro*, versions 232, 238, 245, 255, 265, 275.

3 Résumé

Les systèmes *Xerox Workcentre* sont des imprimantes embarquant des fonctions de photocopie, de numérisation, de courrier électronique et de télécopie. Plusieurs vulnérabilités dans les produits affectés permettent à un utilisateur malintentionné d'accéder à des données sensibles et d'exécuter un code arbitraire à distance.

4 Description

De multiples vulnérabilités affectent les systèmes *Xerox Workcentre* et *Xerox Workcentre Pro* :
- une faille de l'autoconfiguration permet à l'attaquant de modifier la configuration ;
- un défaut de gestion des permissions permet l'accès à des systèmes vulnérables ;
- un manque de validation des entrées dans l'interface web permet de l'injection de commandes ;
- des requêtes peuvent être acceptées en HTTP alors qu'elles ne devraient l'être qu'en HTTPS ;
- une erreur dans la fonction de numérisation permet d'accéder à des fichiers sécurisés ;
- une erreur dans la fonction de courrier électronique permet le détournement de signature ;
- l'heure système peut être incorrecte, donc celle inscrite dans les journaux également.

5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité XEROX XRX-06-006 du 30 novembre 2006 :
  http://www.xerox.com/dowloads/usa/en/c/cert_XRX_06_006_v1.pdf

Gestion détaillée du document

01 décembre 2006 version initiale.